IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
UTILITY PATENT APPLICATION TRANSMITTAL
UNDER 37 CFR 1.53(b)

Address to:	Attorney Docket No.	TU999033
Assistant Commissioner for Patents	Inventor(s)	**JONATHAN WADE AIN, et al.**
Box Patent Application	Express Mail Label No.	
Washington, DC 20231	Total Pages	38

Title of Application:

FIBRE CHANNEL ADDRESS BLOCKING

Transmitted with the patent application are the following:

29 Page(s)	Specification, claims, abstract
5 Page(s)	Informal drawing sheets
2 Page(s)	Declaration and Power of Attorney
1 Page(s)	Recordation of Assignment
1 Page(s)	Assignment of the Invention to International Business Machines Corporation
___ Page(s)	Information Disclosure Statement (IDS) (citation copies not included in number of pages)
___ Page(s)	Preliminary Amendment

This application is a: ___ Continuation ___ Divisional ___ Continuation-in-Part of prior application Serial No. ___ _____, filed on_____.

Fee Calculation

	Claims Filed		Extra	Rate	Fees
Basic Fee					$760.00
Total Claims	10	-20 =	-0-	x$18.00	
Independent Claims	9	-3 =	-6-	x$78.00	$468.00
Multiple Dependent Claim				+ $260.00	
				Assignment	
				TOTAL	$1228.00

_X_ Please charge my Deposit Account No. **09-0449** in the amount of **$ 1228.00**.
A duplicate copy of this sheet is attached.

_X_ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account **09-0449**. A duplicate copy of this sheet is attached.

_X_ Any filing fees under 37 CFR 1.16 for the presentation of extra claims.

_X_ Any patent application processing fees under 37 CFR 1.17.

Respectfully submitted,
JONATHAN WADE AIN, et al

Robert M. Sullivan (Reg. #39,391)
Attorney for Applicant
Telephone: 520-799-2550
From: IBM Corporation
Intellectual Property Law
9000 S. Rita Road (90A/9032)
Tucson, Arizona 85744

/rm

TU999033

FIBRE CHANNEL ADDRESS BLOCKING

BACKGROUND OF THE INVENTION

1. Technical Field

The invention relates to fibre channel computer networks and more particularly to apparatus and method for preventing unwanted access to data at a target device when an invalid source address is detected.

2. Description of the Prior Art

Fibre channel is a general name of a new protocol for flexible information transfer. The fibre channel provides a high speed transfer of large amounts of information while providing an interconnection for various interfaces such as central processing units and data storage devices. The fibre channel permits the transporting of multiple protocols over a common physical interface. The channel protocol refers to a peripheral input/output interface to a host computer that transports large amounts of data between the host computer and the peripheral device such as a data storage system. Data transfer is handled in hardware with little or no software involvement once an input/output operation begins. A network protocol on the other hand usually supports host-to-host communication and refers to an input/output interface that usually supports many small transactions. Fibre channel provides an input/output interface that meets the needs of channel protocol and network protocols.

The fibre channel while increasing the number of devices that can be interconnected is unaware of the content or meaning of the information being transmitted on the channel. The fibre channel also increases the allowable distance between devices and increases the transfer rate of the data. This becomes a problem when one user wants to protect its private data from access from the remainder of the network. Many requests for data can be transmitted on a fibre channel and many sources of data can be connected to the return path of the fibre channel. Thus, unauthorized requests for private data can be made from anyone of the multiple requesters connected to a fibre channel. It is, therefore, an object of the present invention to provide an apparatus and a method for protecting data sources from access by unauthorized requesters.

It would be advantageous to provide a network security technique that permits fibre channel interconnection to a worldwide network while protecting a user's private data from access without authorization.

SUMMARY OF THE INVENTION

The invention provides a technique that permits network access to a storage device while monitoring the source address of the requester to determine whether the requester has been authorized to access the data. A blocking device is positioned between the fibre channel address target and the fabric switch controlling the connection of the source and the target. The blocker inspects all incoming frames of data. The blocker checks the source and destination addresses. If a frame of data is detected that is addressed to an unconfigured source/destination address peer, the frame has its data replaced with IDLE characters. The source could be a host computer requester with a private data storage device being the target. Likewise, the source could be the private data storage with the target being the host computer of the requester. With this invention, unauthorized data is prevented from being transported along the fibre channel while the integrity of the transmission of data is maintained by transporting IDLE characters instead of data frames of information.

The invention provides a number of distinct advantages. The present invention provides apparatus that is positioned in the fibre channel to block either an unauthorized access to private data or to prevent the unauthorized access to a user's network from external network addressing. The invention is unique in that the integrity of the fibre channel is not disturbed since the data frames are replaced by IDLE characters and thereby the transmission along the fibre channel is not interrupted. In the method of the invention, the destination target address is compared to an allowed list of addresses. If a valid comparison is made, the data frame is passed along the fibre channel. If there is no comparison, as would be the case for an unauthorized access, the data frames are converted to IDLE characters and

transmitted down the fibre channel. The blocking apparatus of this invention can be positioned to prevent unauthorized access to either a private data source or the entire private user's network.

An object of the present invention, therefore, is to provide an enhanced fibre channel network.

Another object of the present invention is to provide a means and a process to prevent unauthorized access to data through a fibre channel.

Still another object of the present invention is to provide apparatus and an article of manufacture that maintains the integrity of the fibre channel by replacing the data frames with IDLE characters and thereby continuing the data flow along the channel.

The foregoing, and other objects, features and advantages of the invention will become more apparent to those skilled in the art after considering the following detailed description in connection with the accompanying drawing in which reference numbers designate like parts throughout.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of the hardware components and interconnection of one illustrative implementation of the invention;

FIG. 2 is a block diagram of the hardware components and interconnections of a second illustrative implementation of the invention;

FIG. 3 is a block diagram of the apparatus of the invention as inserted in a fibre channel;

FIG. 4 is a detailed block diagram of the apparatus of the present invention as shown in FIG. 3; and

FIG. 5 is a flowchart showing a sequence of steps to control the unauthorized accessing of data while maintaining the integrity of the fibre channel in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The invention concerns the address blocking in a fibre channel that blocks access by an unauthorized user to confidential data of a second user in a network. The frames of data being transmitted down the fibre channel is inspected incoming to the device that is to be protected. In one embodiment of the invention, the blocking device is placed between a private data storage system and the fibre switch of the user holding the confidential data in his private storage system. In a second embodiment of the invention, the blocking device is placed between the fibre switch of the confidential data owner and the confidential owner's network adapter used to access the fibre channel network to the outside world. The blocker includes a comparator that checks the source and authorized addresses thereby permitting access to the owner's private data storage only to authorized users. The blocking device also checks the transmission of data from the private data storage back to the user and again compares the source of authorized addresses. The frames of data in both regulating devices replace the data frame with IDLE characters. The present invention also includes a method for converting the data frames to IDLE characters according to the present invention. For an overview of the fibre channel, reference is made to the book entitled, "The Fibre Channel Bench Reference" by Jeffrey D. Stai, published by the ENDL Publications of Saratoga, California and copyrighted 1996-1999. The book gives an overview of the fibre channel arbitrated loop (FCAL) topology and the fabric switching configurations used in fibre channels. Further details of the fibre channels can be obtained from this book and is useful for

understanding the present invention. An overview of the FCAL topology and the use of the invention as positioned between a FCAL target and the interconnection is shown in FIG. 1.

Referring now to FIG. 1, a FCAL system is used as the internal system 10 interconnected with a fabric switch 12. The fabric switch 12 is shown connected to two public work stations 14 and 16 but it should be understood that the showing of two does not limit the number of public work stations that can be interconnected with a fabric switch. The internal FCAL system can include one or more private work stations 18, one or more public data storage systems 20, and one or more private data storage systems 22. The ports of each of the private workstation 18, the public data storage 20, and the private data storage 22 are interconnected in an arbitrated loop represented by the hub 24. A controller 26 operates and controls the interconnectivity of the different systems in the internal FCAL system by controlling the operation of the hub 24. A blocker 30, representing the present invention, is shown positioned between the hub 24 and the private data storage 22. The blocker 30 protects unauthorized access to the private data storage 22 of the internal FCAL system 10. This could happen, for instance, if the public workstation 14, for instance, requests access to the private data storage 22 through the fabric switch 12 and into the internal FCAL system 10 by virtue of loop connection to the hub 24. The blocker 30 prevents unauthorized access to the private data storage system if there is an unauthorized request for access outside of the internal FCAL system. The blocker 30 inspects all incoming frames of data, checks the source and destination addresses included in the frames of data and prevents the access to the private data storage 22 if the user frame is detected that is addressed to an unconfigured source/destination

addressed pair, the frame is replaced with IDLE characters and, therefore, the frame is never transmitted to the private data storage 22. A second embodiment in use of the blocker 30 is shown in FIG 2.

Referring now to FIG. 2, an internal FCAL system 100 is shown including a private workstation 102, a public data storage 104 and a private data storage 106 all interconnected to a FCAL loop technology in a hub 108. The blocker 30 of the present invention is shown positioned between a fabric switch 110 and the internal FCAL system 100 on an input fibre channel 112. The fibre switch 110 is shown interconnected through fibre channels to a plurality of public workstations 114. The fabric switch 110 represents an interconnection to many workstations and data storages all external to the internal FCAL system 100. In the embodiment shown in FIG. 2, the invention disclosed in blocker 30 is shown positioned between the incoming fibre channel 112 from the fabric switch 110 and intercepts the frames of data on the fibre channel directed towards the hub 108. In this embodiment, the invention is positioned between the FCAL target represented by the internal FCAL system 100 and the fabric switch 110. As in the first embodiment, the blocker 30 inspects all incoming frames to the internal FCAL system 100 and checks the source and destination addresses included into the data frames on the fibre channel 112. Again, if a user data frame is detected by the blocker 30 on the fibre channel 112 that is addressed to an unconfigured source/destination address pair, the data frame is replaced with IDLE characters and thereby no access is permitted by an unauthorized user of the data whether public or private located in the internal FCAL system 100. A block diagram of the blocker 30 of the embodiments of FIGs 1 and 2 is shown in FIG. 3.

In FIG. 3, the blocker 30 is shown positioned between a hub 120 and a FCAL target 122. The hub 120 represents the hub 24 of the first embodiment in FIG. 1 and it represents the fabric switch 110 in the second embodiment of FIG. 2. The FCAL target 122 represents the private data storage 22 of the FIG. 1 embodiment and the internal FCAL system 100 in the embodiment of FIG. 2. The blocker 30 includes a decoder 32 for receiving the serial data on the fibre channel from the hub 120. The serial data is converted to parallel words in the decoder 32. The parallel data is placed into a regulator 34 and is also directed to a compare circuit 36. The compare circuit 36 compares the parallel data from the decoder 32 and will compare the data address received to a group of permitted addresses as shown in block 38. If the addresses received by the compare circuit 36 compares to the permitted addresses received from block 38, the trigger 40 circuit triggers the regulator 34 to pass the data frame to an encoder circuit 42 for transmission to the FCAL target 122. Thus if a comparison is made, the trigger 40 allows the regulator 34 to pass the data through an encoder 42 and permits the access to the FCAL target 122. However, if the compare circuit 36 does not detect the receipt of a permitted address from the block 38, the trigger 40 signals the regulator 34 to create IDLE characters and access is prevented to the FCAL target 122. A more detailed outline of the circuitry of blocker 30 is shown in FIG. 4.

In FIG. 4 further details of the blocker 30 is shown. The fibre channel address blocker 30 is built including three primary sections. A transmit/receive section includes a serializer/deserializer (SERDES) chip shown as a serial parallel deserializer 50 and a parallel to serial serializer 52 together with a decoder 54 and an encoder 56. The deserializer 50 receives serial data along a fibre channel 58 and converts the

serial data into ten bit parallel words. The parallel words from the deserializer 50 are directed to the decoder 54 which decodes the ten bit words and packages them in groups of four as 32-bit words with a parity bit for each byte of the word. These 32-bit words are characterized as frame data and include control characteristics that are received within the most significant bits of the 32-bit words. The decoder 54 and the encoder 56 are typically a TQ9303 chip.

The output of the decoder 54, the frame data comprising 32-bit parallel words, are directed to a data first in/first out block, the data FIFO 68. The data FIFO 68 is the second primary section of the fibre channel address blocker 30. The data FIFO 68 is 37 bits wide, 32 bits of data, 4 bits of parity and one bit which carries the control signal so that each frame word can be tracked as data or control. The remaining primary section of the blocker 30 is the control logic section which includes a compare #1 60, a compare #2 circuit 62, an AND gate 66 and a multiplexor 70. The blocker 30 also includes a target address store 72 and an allowed source addresses store 74. An IDLE character generator 76 is included for directing IDLE characters into the system as needed to block the access to the data of the FCAL target 122. In FIG. 4, serial data transfer is represented by a thin line, and parallel data transfer is represented by a bold line.

As serial data is received along the fibre channel 58 from the hub 120, it is directed to the deserializer 50 and the decoder 54 where the data is converted into parallel data and moved into the first location of the data FIFO 68. The first FIFO location is called the source address S Addr 78. When the next clock cycle occurs, the first data word is shifted into the second FIFO location, the destination identification D Addr 80. A new word is shifted into the first FIFO location S Addr 78. At the next clock cycle, the first word is shifted into the second

FIFO location, a new word is shifted into the first FIFO location and the second word is converted into a third FIFO location called the start of frame SOF 82. The shifting of the data through the data FIFO 68 continues as long as the link to the fibre channel 58 is operational with all data and control words moving through the data FIFO 68. The data FIFO 68 and its control logic are contained within an Altera FLEX 10K field programmable logic array (FPGA). The control logic contains a bank of 24-bit registers at which the target addresses and their corresponding allowed initiator addresses are stored.

When a start of frame character word is detected in a data FIFO 68 at SOF 82, the data FIFO 68 is indicating that a new data frame is being received. The start of frame signal is directed to the compare #1 circuit 60. The data word in the second cell, the D Addr 80 contains the frame type within the routing control field and the destination identification data. The frame data from the D Addr 80 is directed to the input of the compare 60. If the frame is determined to be a FC-4 device data frame, the compare 60 compares the destination identification to the target address from the target address store 72 stored in the register bank in the control logic section of the blocker 30. The next 32-bit frame word is now contained in the first location of the data FIFO 68, the S Addr 78 FIFO location. This frame word contains the 24-bit source address and the output of this data FIFO 68 location, the S Addr 78 location, is directed to the compare 2 circuit 62. The compare 62 of the control logic section compares the source address to the allowed addresses as contained in the allowed address store 74. If the destination address from location 80 of the data FIFO 68 is found to match a target address from the target address store 72, the compare #1 circuit 60 permits a comparison in the compare #2 circuit 62 of the source address from the FIFO location 78 to the allowed

addresses from the allowed address store 74. If a match is found, the compare 62 of the control logic allows the frame data to continue through the data FIFO 68 for transmittal via the Mux 70 to the FCAL target 122. If the destination address from the FIFO location 80 of the data FIFO 68 is not found in the list of target addresses from the target address store 72, the frame is allowed to pass through the data FIFO 68, the encoder 56 and the serializer 52, and is transmitted to the FCAL target 122.

If a match is found for the destination address from the FIFO location 80 in the compare #1 circuit 60, but the source address from the FIFO location 78 is not on the list of allowed addresses from the allowed address store 74, then the compare #2 circuit 62 along the NOT line activates an AND gate 66 which permits the transmission of IDLE characters from the IDLE character generator 76 to be transmitted through the Mux 70, the encoder 56, and the serializer 52, to FCAL target 122 via fibre 84. The control logic of the blocker 30 asserts the IDLE characters, the IDLE characters in turn cause the encoder 56 to ignore the transmit data inputs and to transmit the IDLE characters until an end of frame character is detected in the last FIFO location of the data FIFO 68. This action causes the data frames to apparently disappear.

If the start of frame signal from FIFO location 82 activates the compare #1 circuit 60 and the destination identification from FIFO location 80 matches an address from the target address store 72, the compare #1 circuit 60 activates the compare #2 circuit 62. The activation of the compare #2 circuit 62 causes the comparison of the source address from FIFO location 78 to be compared with the allowed addresses from the allow address store 74 and if again the source address is in the allowed addresses, the NOT line from the compare #2 circuit 62 is directed to the AND gate 66 which allows the transmittal of the data from the

data FIFO 68 to the FCAL target 122 via the encoder 56 and the serializer 52.

The generation of the IDLE characters causes the frames to "disappear", in reality the data frames are replaced by IDLE characters. It should be understood that data frames could be status frames or command frames, that is, any frame that could be a Level FC4 frame.

The control logic section of the blocker 30 is described as particular types of gates and blocks of circuitry to compare address data signals but it should be understood that the control logic described in FIG. 4 is representative of operational steps and should not be limited to the actual logic detail described in FIG. 4. Thus according to the invention, the blocker 30 accepts serial data from a fibre channel, converts the serial data to a parallel data and senses the frame words of the parallel data in order to detect a start of frame signal which then permits the comparison of the destination identification signal to the target address and the comparison of the source address from the incoming data to allowed addresses stored within the blocker 30. If the source address is one of the allowed addresses, the request for data is continued to the FCAL target 122 via the encoder and serializer.

As shown in FIG. 4, the blocker 30 through its control logic section compares the serialized data from the fibre channel 58 which has been converted to parallel data and transmitted to data FIFO 68, senses a start of frame data which then permits a comparison of the destination identification to the target address and a comparison of the source address to the addresses permitted access to the FCAL target 122. If the destination address has sensed and location 80 of data FIFO 68 is found to match the target address from the target address store 72 then the control logic compares the source address to the list of

allowed addresses from the allowed address store 74. If a match is found with the list of allowed addresses, the control logic allows the data frame to continue through the data FIFO 68 for transmission to the FCAL target 122. If a match is found for the destination address but the source address is not on the allowed list of addresses from the allowed address store 74, then the control logic causes the IDLE character generator to generate IDLE characters to the FCAL target 122. The IDLE characters are generated and transmitted until an end of frame character is detected in the last location of the data FIFO 68. This action essentially causes the frames of data to disappear by being substituted by IDLE characters. The data frames that travel through the data FIFO 68 and are not blocked are directed to an encoder and a parallel to serial converter to be encoded into the serial form for transmission through a fibre channel to the target 122.

The decoder 54 and the encoder 56 are typically TQ9303 encoder/decoder (ENDEC) chips. The serial parallel deserializer 50 and the parallel to serial serializer 52 are typically a Triquint fibre channel chip set and form the receive/transmit section of the blocker 30. The serial to parallel deserializer 50 is typically a TQ9502 chip which is a serializer/deserializer (SERDES) chip. The parallel to serial serializer 52 is typically a TQ 9501 serializer chip which converts the parallel words from the encoder 56 into a serial stream to be transmitted on the fibre channel 84 to the target 122.

The control logic pseudo code for the control section of the blocker 30 is as follows. Referring to FIG. 4, if the FIFO location 82 is equal to a start of frame (SOF) and the FIFO location 78 includes a control signal in the source identification that the requesting frame contains an FC4 device data frame type;

AND

FIFO location 80 does not contain a destination identification that compares to the target address;

OR

If FIFO location 82 is equal to a start of frame and FIFO location 82 includes a control signal that the requesting device contains FC 4 device data frame type and the source address from the FIFO location 78 successfully compares to the allowed address in the compare #1 60;

THEN

Allow access to target until the FIFO location 82 signals an end of frame data (EOF);

OTHERWISE

If the FIFO location 82 is equal to a start of frame (SOF) and the FIFO location 80 includes a control signal that the requesting device contains FC4 device data frame type;

AND

The source address from the FIFO location 78 does not successfully compare to the allowed addresses;

THEN

Assert IDLE characters until the FIFO location 82 signals an end of frame (EOF) signal.

A flowchart for the fibre channel address blocking method and process according to the present invention is shown in FIG. 5. Referring to FIG. 5, a block 201 shows that data is received from a hub which could be a fibre channel arbitrated loop or a fabric switch and directed to a serial to parallel conversion such as shown in block 202. The data from the serial to parallel conversion block 202 is directed to a decode to frame data word as shown in a block 204. The parallel data from the frame word is then entered into a first in first out (FIFO) circuit as shown in a block 206. The next step is a decision block where a start

of frame is detected or not as shown in decision block 208. If a start of frame word is not detected the NO line is taken to a block 210 where a sensing of the FIFO frame word is continued and the word is transmitted. If the start of frame word is detected, the flow continues from decision block 208 along the YES line to a block 216 where the data frame type, the target address, and the allowed source addresses are presented from the FIFO as represented by blocks 216, 218 and 220 respectively. If any of the compares fail in decision blocks 216, 218, or 220, the flow reverts to the start block 200. If all three compares are satisfied, that is, that an FC4 device data frame type is detected, and the target address matches the destination address in the FIFO, and the source address is not found on the list of allowed addresses, then the flow goes to block 222, and the multiplexer is switched to transmit IDLE characters.

The flow then goes to a decision block 224 where the end of frame (EOF) character is detected. If in decision block 224, an end of frame character is not detected, then the word is encoded in a block 226, serialized in a block 228, and transmitted to the target as hown in a block 230. The flow goes to the decision block 224 again to check the next word for the end of frame character. If an end of frame (EOF) character is detected, the EOF character is encoded in a block 232, serialized in a block 234, and transmitted to the target via fibre as shown in a block 236. The flow then goes to a block 238, where the multiplexer is switched to normal transfer mode, where data from the FIFO is transmitted in a normal fashion. The flow then reverts back to the START block 200.

Thus, what has been disclosed in the present invention is a method, apparatus, and article of manufacture for blocking a fibre channel address request wherein the incoming frames are inspected and checked for the source and destination addresses.

If the address is authorized, the request is completed and the frame is transferred to the requesting device. If the address detected is from an unconfigured source/destination address, the frame is replaced with IDLE characters to prevent any transfer of unauthorized data to the requester.

Using the foregoing specification, the invention may be implemented as a machine, process, or article of manufacture by using standard programming or engineering techniques to produce computer software, firmware, hardware, or a combination thereof. Any resulting programs may be embodied within one or more computer usable media such as memory devices or transmitting devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "article of manufacture" and "computer program product" as used in the following claims are intended to encompass a computer program existing on any memory device or in any transmitting device. Memory devices include fixed (hard) disk drives, diskettes, optical disks, magnetic tape, and semiconductor memories such as ROM, PROM, etc. Transmitting devices include the internet, electronic bulletin board and message/note exchanges, telephone/modem-based network communication, hard-wired/cable communication network, cellular communication, radio wave communication, satellite communication, and other stationary or mobile network systems and communication links. A computer program product as described above may be used by transmitting it via any of the foregoing transmitting devices.

One skilled in the art of computer science will easily be able to combine the software created as described with appropriate general purpose or special purpose computer hardware to create a computer system and/or computer subcomponents embodying the invention and to create a computer system and/or

computer subcomponents for carrying out the method of the invention.

Although the invention is described here and with reference to the preferred embodiments, one skilled in the art will readily appreciate that other apparatus, methods and applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention. For example, specific chips and chips that are described herein together with representative logic items. The disclosure of specific items should not limit the invention and accordingly, the invention should only be limited by the claims below.

We claim:

1. Apparatus for blocking an unauthorized access to limited access data stored in a fibre channel configuration network system including a fabric switch fibre channel interconnecting work stations and data storage devices with an internal fibre channel arbitrated loop having internal work stations and internal data storage systems, at least one internal data storage system containing the limited access data stored therein, said blocking apparatus intercepting data access to the internal data storage system containing the limited access data, said blocking apparatus comprising:

a receiving section means for receiving a serialized request for data from a requesting source on a fibre channel from the fabric switch and for transforming the serial data to parallel frames of data;

a FIFO section for sequentially receiving sets of parallel frames of data from said receiving section and for transmitting the parallel sets of data to the target after reserialization;

a control section including means for individually sensing each set of parallel frames of data from said FIFO section, means for sensing a start of data frame from one set of the parallel frames of data, means for comparing individual sets of parallel frames of data from said FIFO section after sensing the start of frame data to compare another set of frame data from said FIFO section to allowed addresses stored in said control section, and means for generating IDLE characters representing no data, said control section permitting the transmission of parallel sets of data frames to the target data store if said comparing means senses a match between the allowed addresses and the set of parallel frame of data in said FIFO section and activating the

generating means to transmit IDLE characters if no match is sensed; and

a transmitting section under control of said control section to encode and serialize the parallel sets of data received from the FIFO, or to transmit the IDLE characters if no match is sensed.

2. Blocking apparatus positioned between a target data storage and a hub in a fibre channel arbitrated loop system for stopping the unauthorized transmittal of data from the target data storage to a requesting source, said blocking apparatus comprising:

a receiving section means for receiving a serialized request for data from the requesting source on a fibre channel and for transforming the serial data to parallel frames of data;

a FIFO section for sequentially receiving sets of parallel frames of data from said receiving section and for transmitting the parallel sets of data to the target data store;

a control section including means for individually sensing each set of parallel frames of data from said FIFO section, means for sensing a start of data frame from one set of the parallel frames of data, means for comparing individual sets of parallel frames of data from said FIFO section after sensing the start of frame data to compare another set of frame data from said FIFO section to allowed addresses stored in said control section, and means for generating IDLE characters representing no data, said control section permitting the transmission of sets of data frames after serialization to the target if said comparing means senses a match between the allowed addresses and the set of parallel frame of data in said FIFO section and activating the generating means to transmit IDLE characters if no match is sensed; and

a transmitting section under control of said control section to encode and serialize the parallel sets of data received from the FIFO section if said comparing means senses a match or to transmit the IDLE characters if no match is sensed.

3. Blocking apparatus positioned between a fabric switch system and a hub in a fibre channel arbitrated loop system for stopping the unauthorized transmittal of data from the hub to a requesting source in the fabric switch system, said blocking apparatus comprising:

a receiving section means for receiving a serialized request for data from the requesting source on a fibre channel from the fabric switch and for transforming the serial data to parallel frames of data;

a FIFO section for sequentially receiving sets of parallel frames of data from said receiving section and for transmitting the parallel sets of data to the target after serialization;

a control section including means for individually sensing each set of parallel frames of data from said FIFO section, means for sensing a start of data frame from one set of the parallel frames of data, means for comparing individual sets of parallel frames of data from said FIFO section after sensing the start of frame data to compare another set of frame data from said FIFO section to allowed addresses stored in said control section, and means for generating IDLE characters representing no data, said control section permitting the transmission of sets of data frames after serialization to the target if said comparing means senses a match between the allowed addresses and the set of parallel frame of data in said FIFO section and activating the generating means to transmit IDLE characters if no match is sensed; and

a transmitting section under control of said control section to encode and serialize the parallel sets of data received from the FIFO section if said comparing means senses a match or to transmit the IDLE characters if no match is sensed.

4. Blocking apparatus positioned between a target data storage and a hub in a fibre channel arbitrated loop system for stopping the unauthorized transmittal of data from the target data storage to a requesting source, said blocking apparatus comprising:

a serial-to-parallel receiving means connected to a fibre channel for receiving a serialized request for data from the requesting source on the fibre channel and for transforming the serial data to groups of parallel data;

an encoding means for packaging groups of parallel data from said receiving means into a series of set of parallel frames of data;

a FIFO section for sequentially receiving and storing sets of parallel frames of data from said encoding means;

a control section including an allowed addresses store, an allowed address comparing means, means for individually sensing each set of parallel frames of data from said FIFO section, means for sensing a start of data frame from one set of the parallel frames of data, and means for generating IDLE characters representing no data,

said allowed address comparing means comparing individual sets of parallel frames of data from said FIFO section after sensing the start of frame data to compare a source address set of frame data from said FIFO section to an address stored in said allowed addresses store;

said control section permitting the transmission of parallel sets of data frames from said FIFO section to the target after serialization if said allowed address comparing means senses a

match between the allowed addresses and the set of parallel frame of data in said FIFO section and activating the generating means to transmit IDLE characters if no match is sensed;

an encoder connected to receive either the data frames from the FIFO section or the IDLE characters from the IDLE character generator and to convert the data frames to smaller groups of parallel words; and

a parallel to serial converter connected to said encoder to change the parallel words from said decoder to serial data for transmission on the fibre channel to the target.

5. Blocking apparatus as described in **Claim 4** wherein said control section further includes means for storing a target address and a target address comparing means, said target address comparing means comparing the target address from said target address store of a destination identification set of parallel frame of data from said FIFO section, said target address comparing means activating said allowed address comparing means if a match is made in the target address comparing means to compare the allowed address from the allowed addresses store of the source address set of parallel frame data from the FIFO section, said control section permitting the transfer of data frames from the FIFO section to the target if the target address comparing means does not match the target address to the source address set of frame data from the FIFO section.

6. A method for blocking an unauthorized access to limited access data stored in a fibre channel configuration network system including a fabric switch fibre channel interconnecting work stations and data storage devices with an internal fibre channel arbitrated loop having internal work stations and internal data storage systems, at least one internal data storage

system containing the limited access data stored therein, said method intercepting data access to the internal data storage system containing the limited access data, said method comprising the steps of:

accepting serial data from a fibre channel connected to a hub;

converting the serial data to parallel data;

encoding the parallel to frames of data;

sequentially entering the parallel frames of data into word of data in a FIFO store;

detecting a start of word data in the FIFO store;

sensing an upper level device path word from the FIFO store;

comparing the destination identifying address to a target address;

comparing a source address word from the FIFO store if the destination identifying address matches the target address, otherwise enabling the transfer of the frame word to the target;

comparing a source address word from the FIFO store to allowed addresses stored in an allowed address store;

enabling the transfer of frame data from the FIFO to the target if a match is sensed, otherwise, enabling the generation of IDLE characters; encoding the generated IDLE characters and the data from the target into parallel data;

converting the parallel data into serial data; and

directing the serial data signals to a fibre channel.

7. A method for blocking an unauthorized access to limited access data stored in a fibre channel configuration network system including a fabric switch fibre channel interconnecting work stations and data storage devices with an internal fibre channel arbitrated loop having internal work stations and internal data storage systems, at least one internal data storage

system accessed by a target address and containing the limited access data stored therein, said method intercepting data access to the internal data storage system containing the limited access data, said method comprising the steps of:

accepting serial data from the fabric switch fibre channel;

converting the serial data to parallel data;

decoding the parallel data to parallel frames of data;

sequentially entering the parallel frames of data into words of data in a FIFO store;

detecting a start of word data in the FIFO store;

sensing an upper level device path word from the FIFO store;

comparing the destination identifying address from the fibre channel data to the internal target address;

comparing a source address word from the FIFO store to allowed addresses stored in an allowed address store if the destination identifying address matches the internal target address, otherwise enabling the transfer of the frame word to the internal target data storage system;

enabling the transfer of frame data from the FIFO to the target if a match is sensed between the source address and the target address, otherwise, enabling the transmission of IDLE signals; and

encoding the IDLE signals or the data signals from the FIFO store into parallel signals;

converting the parallel signals into serial data; and

directing the serial data signals to a fibre channel.

8. A method for blocking an unauthorized access to limited access data stored in a fibre channel configuration network system including a fabric switch fibre channel interconnecting work stations and data storage devices with an internal fibre channel arbitrated loop having internal work stations and

internal data storage systems, at least one internal target data storage system accessed by a target address and containing the limited access data stored therein, said method intercepting data access to the internal target data storage system containing the limited access data, said method comprising the steps of:

accepting data from the fabric switch fibre channel;

comparing a destination identifying address from the fibre channel data to the internal target address;

comparing a source address from a requesting device in the fabric switch fibre channel to allowed addresses stored in an allowed address store if the destination identifying address matches the internal target address, otherwise enabling the transfer of the source address to the internal target data storage system;

enabling the transfer of information from the requesting device to the internal target data storage system if a match is sensed between the source address and the target address otherwise, enabling the generation of IDLE characters; and

directing the IDLE characters or the data frames from the internal target data storage system to a fibre channel of the fabric switch fibre channel.

9. An article of manufacture for use in a fibre channel configuration network system including a fabric switch fibre channel interconnecting work stations and data storage devices with an internal fibre channel arbitrated loop having internal work stations and internal data storage systems, at least one internal data storage system accessed by a target address and containing the limited access data stored therein, said method intercepting data access to the internal data storage system containing the limited access data,

said article of manufacture comprising a computer-readable storage medium tangibly embodying a program of executable computer instructions which may cause said fibre channel configuration network to:

accept serial data from the fabric switch fibre channel;

convert the serial data to parallel data;

decode the parallel data to parallel frames of data;

sequentially enter the parallel frames of data into words of data in a FIFO store;

detect a start of frame word data in the FIFO store;

sense an upper level device path word from the FIFO store;

compare the destination identifying address from the fibre channel data to the internal target address;

compare a source address word from the FIFO store to allowed addresses stored in an allowed address store if the destination identifying address matches the internal target address, otherwise enable the transfer of the frame word to the internal target data storage system;

enable the transfer of frame data from the FIFO to the internal target data store if a match is sensed between the source address and the target address, otherwise, enable the transmission of IDLE characters;

encode the IDLE signals or the data signals from the internal target data store into parallel signals;

convert the parallel signals into serial data; and

direct the serial data to a fibre channel of the fabric switch fibre channel.

10. An article of manufacture for use in a fibre channel configuration network system including a fabric switch fibre channel interconnecting work stations and data storage devices with an internal fibre channel arbitrated loop having internal

work stations and internal data storage systems, at least one internal target data storage system accessed by a target address and containing the limited access data stored therein,

said article of manufacture comprising a computer-readable storage medium tangibly embodying a program of executable computer instructions which may cause said fibre channel configuration network to intercept data access to the internal target data storage system containing the limited access data, said article of manufacture to:

accept data from the fabric switch fibre channel;

compare a destination identifying address from the fibre channel data to the internal target address;

compare a source address from a requesting device in the fabric switch fibre channel to allowed addresses stored in an allowed address store if the destination identifying address matches the internal target address, otherwise enable the transfer of the data frame to the internal target data storage system;

enable the transfer of said data frame from the requesting device to the internal target data storage system if a match is sensed between the source address and the target address otherwise, enable the generation of IDLE signals; and

direct the IDLE signals or the data signals from the internal target data storage system to a fibre channel of the fabric switch fibre channel.

CHANNEL ADDRESS BLOCKING

ABSTRACT OF THE INVENTION

A method and system including apparatus for detecting and blocking an invalid request to a target wherein fibre channels interconnect the data processing configuration. A request made from a hub such as a fabric switch to an internal fibre channel arbitrated loop is blocked by substituting IDLE characters for the frames of data included with the request. The substitution of IDLE signals can also occur within an internal fibre channel arbitrated loop system where access is blocked to a confidential data storage system. If the request is legitimate, the data frames are passed to the target and the requested data is transmitted back to the requester. If the request is refused as being an unauthorized request, the data frames are replaced with IDLE characters and no transfer of confidential data occurs.

TU999033

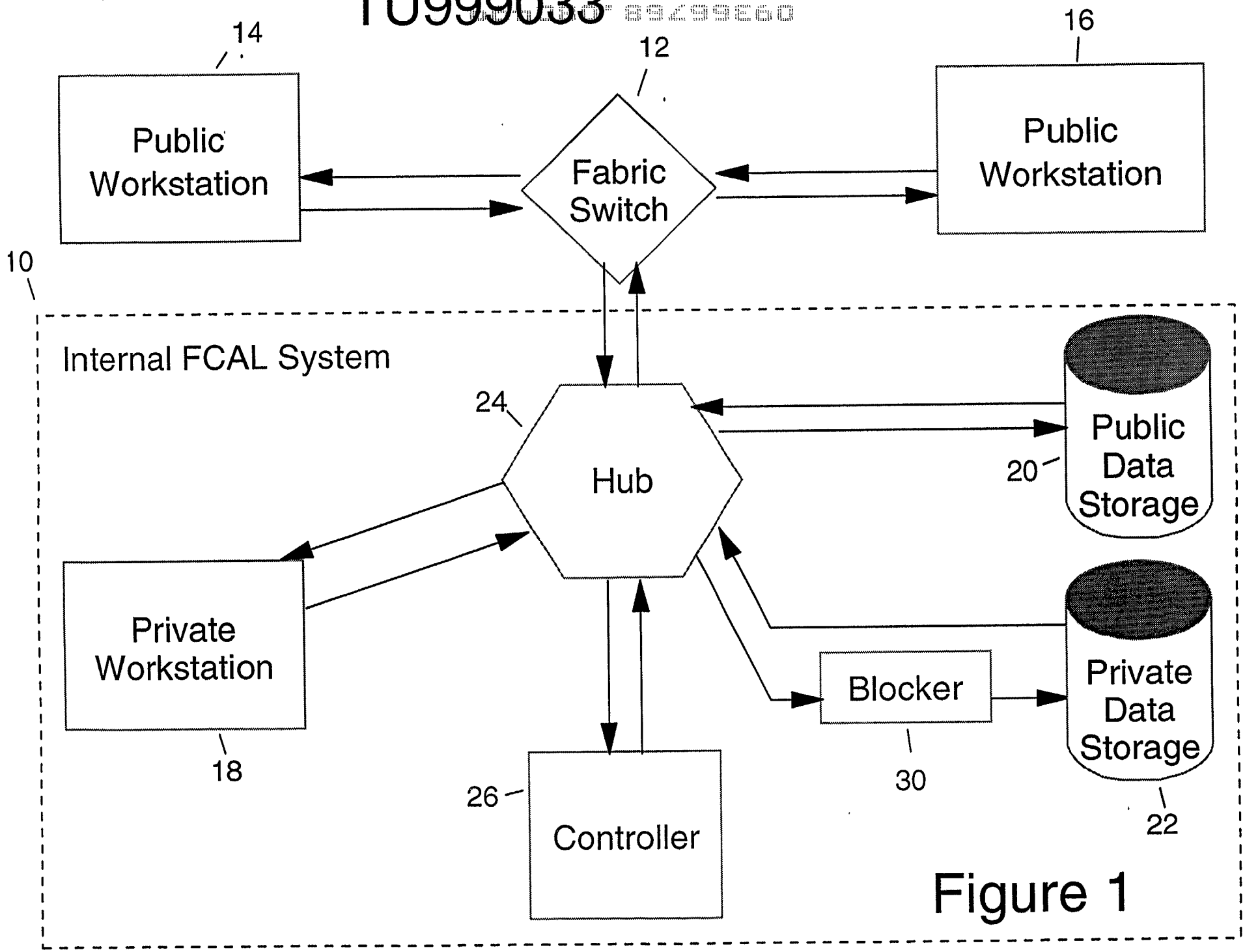
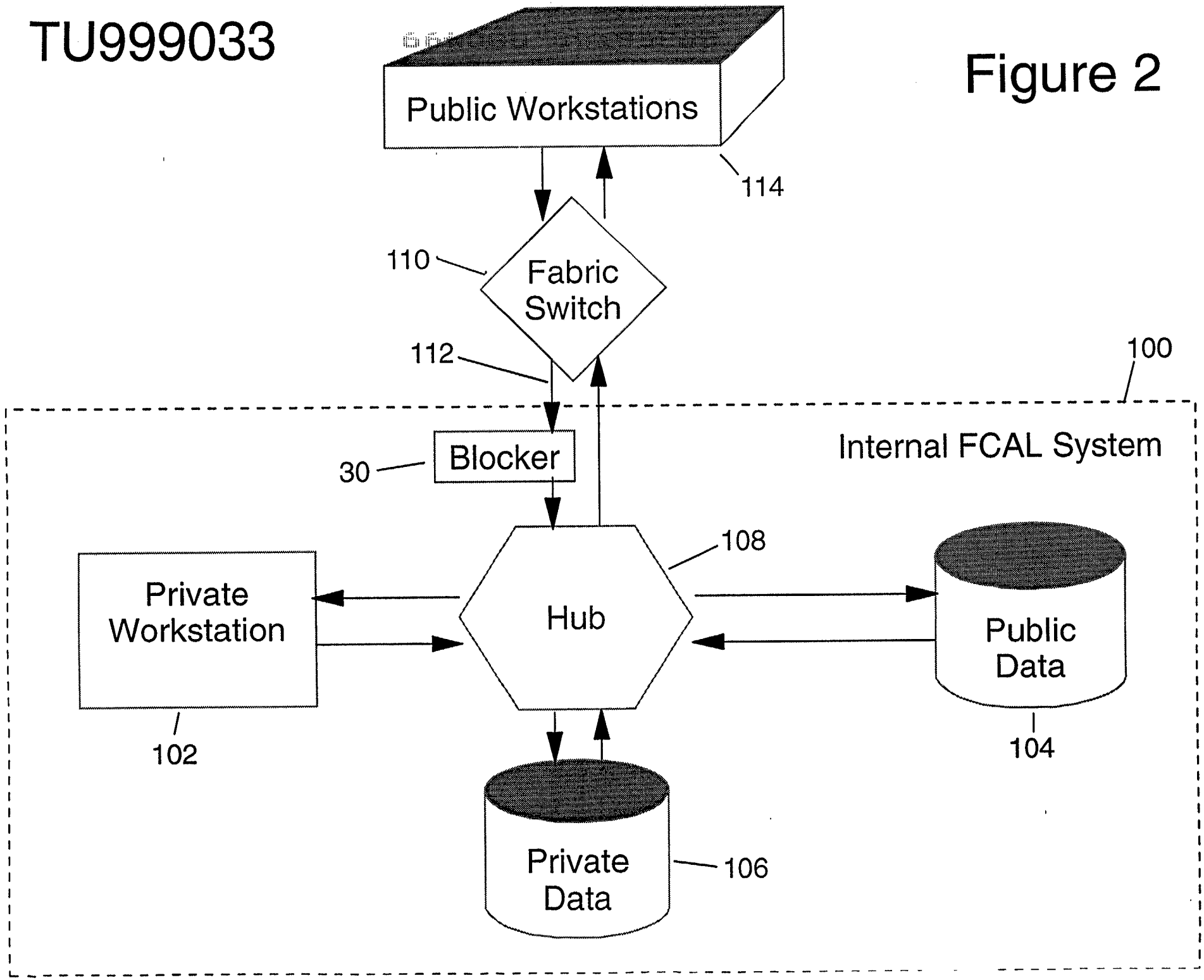


Figure 1

TU999033

Figure 2



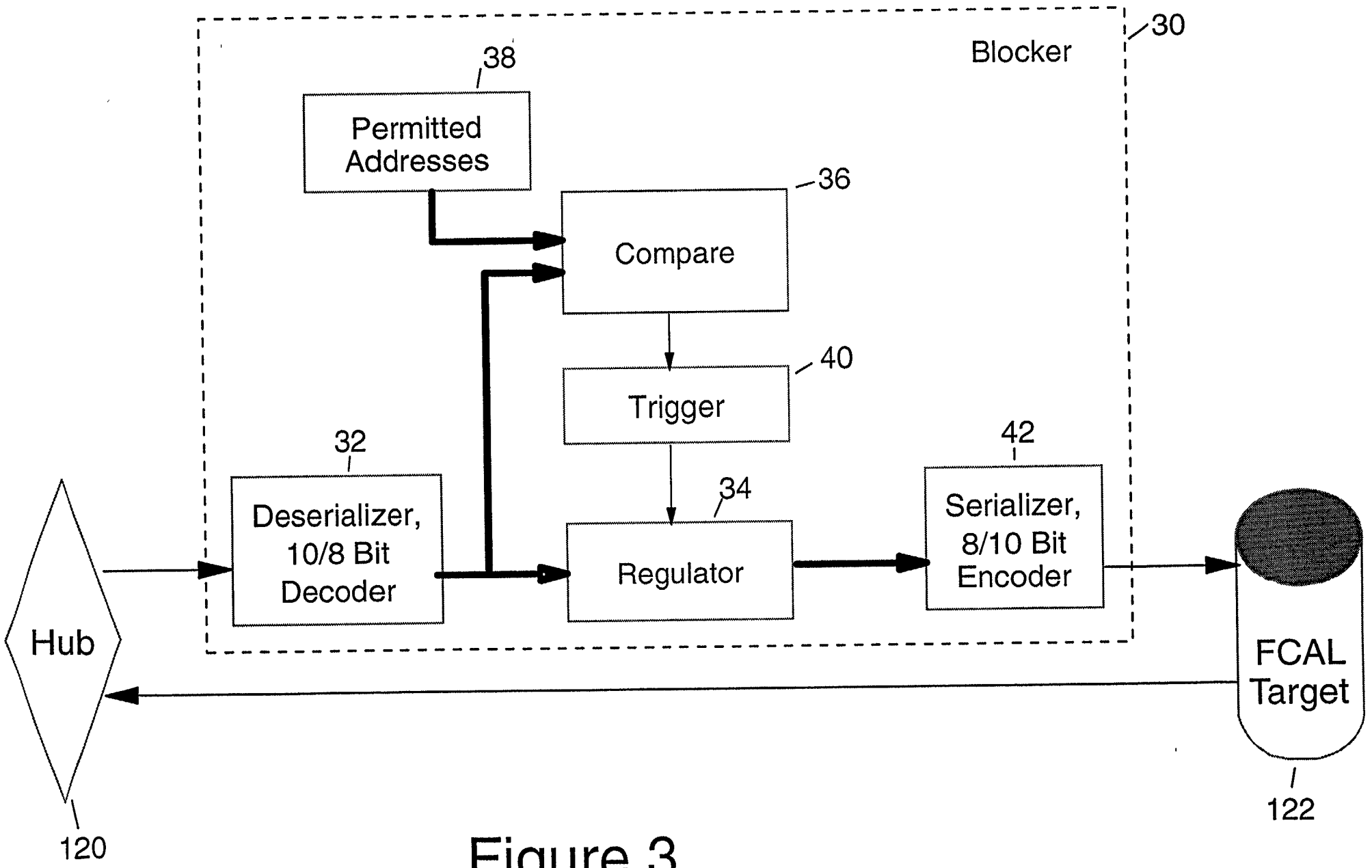

Blocker
30
38
Permitted Addresses
36
Compare
40
Trigger
32
Deserializer, 10/8 Bit Decoder
34
Regulator
42
Serializer, 8/10 Bit Encoder
Hub
FCAL Target
120
122

Figure 3

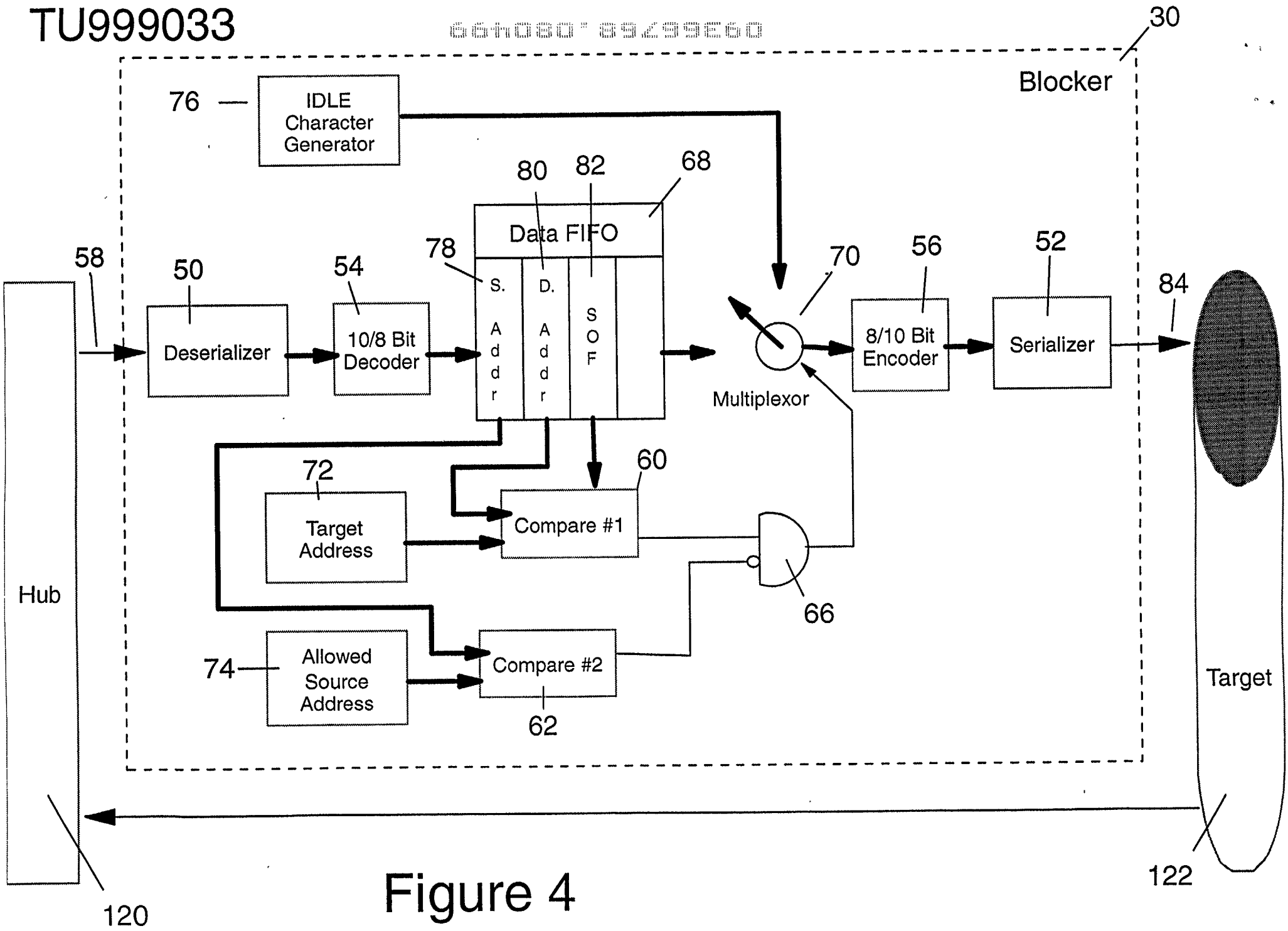

30
Blocker
76
IDLE Character Generator
80
82
68
Data FIFO
78
S. Addr
D. Addr
SOF
58
50
Deserializer
54
10/8 Bit Decoder
70
56
8/10 Bit Encoder
52
Serializer
84
Multiplexor
72
Target Address
60
Compare #1
66
Hub
74
Allowed Source Address
Compare #2
62
Target
120
122

Figure 4

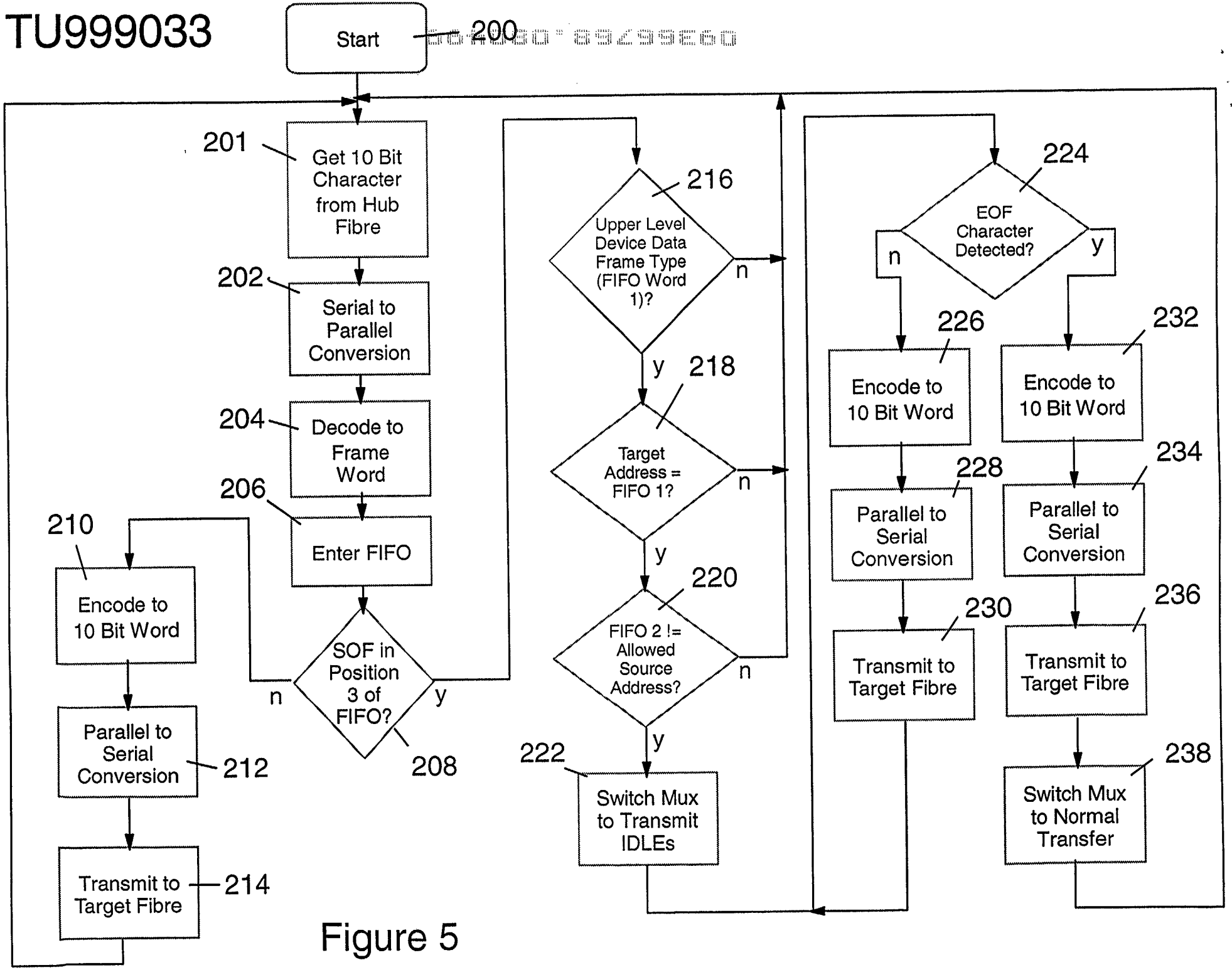

Start
200
201
Get 10 Bit Character from Hub Fibre
202
Serial to Parallel Conversion
204
Decode to Frame Word
206
Enter FIFO
SOF in Position 3 of FIFO?
208
n
y
210
Encode to 10 Bit Word
Parallel to Serial Conversion
212
Transmit to Target Fibre
214
216
Upper Level Device Data Frame Type (FIFO Word 1)?
n
y
218
Target Address = FIFO 1?
n
y
220
FIFO 2 != Allowed Source Address?
n
y
222
Switch Mux to Transmit IDLEs
224
EOF Character Detected?
n
y
226
Encode to 10 Bit Word
228
Parallel to Serial Conversion
230
Transmit to Target Fibre
232
Encode to 10 Bit Word
234
Parallel to Serial Conversion
236
Transmit to Target Fibre
238
Switch Mux to Normal Transfer

Figure 5

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

FIBRE CHANNEL ADDRESS BLOCKING

the specification of which (check one)

_X_ is attached hereto.
___ was filed on _____
as Application Serial No. _____
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
None			___Yes	___No
(Number)	(Country)	(Day/Month/Year Filed)		

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56, which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

None		
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Philip R. Wadsworth (#29,219)
Monica D. Lee (#40,696)
G. Marlin Knight (#33,409)
Paik Saber (#37,494)
Christopher A. Hughes (#26,914)
John E. Hoel (#26,279)
Robert B. Martin (#26,945)
Robert M. Sullivan (#39,391)
Joseph F. Villella, Jr. (#30,599)
Esther E. Klein (#34,337)
Douglas R. Millett (#31,784)
Noreen A. Krall (#39,734)
Edward A. Pennington (#32,588)
Joseph C. Redmond, Jr. (#18,753)
Randall J. Bluestone (#40,518)
James A. Pershon (#24,198)

Send correspondence to:

IBM Corporation
Intellectual Property Law
9000 So. Rita Road (90A/9032)
Tucson, Arizona 85744

Direct Telephone Calls to: (name and telephone number) **James A. Pershon, 520-297-3741**

Full name of sole or first joint-inventor: JONATHAN WADE AIN

Inventor's signature: Jonathan Wade Ain Date: 8/2/99

Residence: **10566 E. Camino Quince, Tucson, Arizona 85748**

Citizenship: **US**

Post Office Address: Same

Full name of second joint-inventor: ROBERT GEORGE EMBERTY

Inventor's signature: Robert George Emberty Date: 8/2/99

Residence: **2 South Antietam Place, Tucson, Arizona 85710**

Citizenship: **US**

Post Office Address: Same

Full name of third joint-inventor: CRAIG ANTHONY KLEIN

Inventor's signature: Craig Anthony Klein Date: 8/2/99

Residence: **780 N. Promontory, Tucson, Arizona 85748**

Citizenship: **US**

Post Office Address: Same